CLAIMS

1. A method for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said originating access device using a second PHY channel; and

hosting said communication session over at least one of said first PHY channel, said second PHY channel and a third PHY channel.

2. The method according to claim 1, further comprising generating at least one encryption/decryption key for use during said communication session.

3. The method according to claim 2, wherein said authenticating further comprises requesting authentication information from an authentication server.

4. The method according to claim 3, wherein said authenticating further comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

5. The method according to claim 4, further comprising delivering said encryption key to said originating access device via one of said first PHY channel or said second PHY channel.

6. The method according to claim 1, further comprising receiving an identification of said originating access device by said access point.

7. The method according to claim 6, wherein said identity of said originating access device is at least one of a WEP key, a MAC address, and an IP address.

8. The method according to claim 1, further comprising acknowledging said received request on said first PHY channel.

9. The method according to claim 1, further comprising determining a type of traffic generated by said originating access device on said first PHY channel.

10. The method according to claim 9, further comprising generating at least one encryption/decryption key dependent on said determined traffic type.

11. The method according to claim 10, further comprising distributing said generated encryption/decryption key via at least one of said second PHY channel and said third PHY channel.

12. The method according to claim 1, further comprising establishing at least one virtual channel between said originating access device and a terminating access device.

13. The method according to claim 12, further comprises tunneling information between said originating access device and said terminating access device.

14. The method according to claim 12, further comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel and said third PHY channel.

15. A machine-readable storage, having stored thereon, a computer program having at least one code section for providing multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said originating access device using a second PHY channel; and

hosting said communication session over at least one of said first PHY channel, said second PHY channel and a third PHY channel.

16. The machine-readable storage according to claim 15, further comprising code for generating at least one encryption/decryption key for use during said communication session.

17. The machine-readable storage according to claim 16, wherein authenticating code further comprises code for requesting authentication information from an authentication server.

18. The machine-readable storage according to claim 17, further comprising code for delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

19. The machine-readable storage according to claim 18, further comprising code for delivering said at least one encryption key to said originating access device via one of said first PHY channel or said second PHY channel.

20. The machine-readable storage according to claim 15, further comprising code for receiving an identification of said originating access device by said access point.

21. The machine-readable storage according to claim 20, wherein said identity of said originating access device is at least one of a WEP key, a MAC address, and an IP address.

22. The machine-readable storage according to claim 15, further comprising code for acknowledging said received request on said first PHY channel.

23. The machine-readable storage according to claim 15, further comprising code for determining a type of traffic generated by said originating access device on said first PHY channel.

24. The machine-readable storage according to claim 23, further comprising code for generating at least one encryption/decryption key dependent on said determined traffic type.

25. The machine-readable storage according to claim 24, further comprising code for distributing said generated encryption/decryption key via at least one of said second PHY channel and said third PHY channel.

26. The machine-readable storage according to claim 15, further comprising code for establishing at least one virtual channel between said originating access device and a terminating access device.

27. The machine-readable storage according to claim 26, further comprises code for tunneling information between said originating access device and said terminating access device.

28. The machine-readable storage according to claim 26, further comprising code for establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel and said third PHY channel.

29. A system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the system comprising:

at least one receiver of an access point adapted to receive on a first PHY channel, a request for initiation of a communication session from an originating access device;

at least one authenticator adapted to authenticate said originating access device using a second PHY channel; and

at least one of said first PHY channel, said second PHY channel and a third PHY channel being adapted to facilitate hosting of said communication session.

30. The system according to claim 29, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key for use during said communication session.

31. The system according to claim 30, wherein said at least one authenticator is adapted to receive requests for authentication information.

32. The system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

33. The system according to claim 32, wherein said at least one authenticator is adapted to deliver said encryption key to said originating access device via one of said first PHY channel or said second PHY channel.

34. The system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point.

35. The system according to claim 34, wherein said identity of said originating access device is at least one of a WEP key, a MAC address, and an IP address.

36. The system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel.

37. The system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel.

38. The system according to claim 37, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key dependent on said determined traffic type.

39. The system according to claim 38, wherein said at least one authenticator is adapted to distribute said generated encryption/decryption key via at least one of said second PHY channel and said third PHY channel.

40. The system according to claim 29, wherein said at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device.

41. The system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device.

42. The system according to claim 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel and said third PHY channel.